Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB04/005179

International filing date: 08 December 2004 (08.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0420159.6
Filing date: 10 September 2004 (10.09.2004)

Date of receipt at the International Bureau: 09 February 2005 (09.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/GB 2004 / 0 0 5 1 7 9

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed Andrew Gerry

Dated 17 January 2005

Patents Form 1/77
Patents Act 1977
(Rule 16)

THE PATENT OFFICE
SA
10 SEP 2004
LONDON

The Patent Office

135EP04 E925259-3 002611
P01/7700 0.00-0420159.6 CHEQUE

Request for grant of a patent

The Patent Office
Cardiff Road
Newport
South Wales NP10 8QQ

1. Your reference
5489402/JAC

2. Patent Application Number
0420159.6 **10 SEP 2004**

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Innovision Research & Technology PLC
Ash Court
23 Rose Street
Wokingham
Berkshire
RG40 1XS

Patents ADP number *(if known)* 8144784001

If the applicant is a corporate body, give the country/state of its incorporation — Country: **England** State:

4. Title of the invention

Protection method for RFID tags

5. Name of agent
"Address for Service" in the United Kingdom to which all correspondence should be sent

Beresford & Co
16 High Holborn
London WC1V 6BX

Patents ADP number 1826001

6. Priority: Complete this section if you are declaring priority from one or more earlier patent applications filed in the last 12 months.

Country	Priority application number	Date of filing

Patents Form 1/77

7. Divisionals, etc: Complete this section only if this application is a divisional application or resulted from an entitlement dispute.

Number of earlier application | Date of filing

8. Is a Patents Form 7/77 (Statement of inventorship and of right to grant of a patent) required in support of this request?

YES

9. Enter the number of sheets for any of the following items you are filing with this form.

Continuation sheets of this form	
Description	6
Claim(s)	3
Abstract	
Drawing(s)	

USA

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents form 7/77)*	1+1 COPY
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for Substantive Examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application

Signature _____ Date 10 September 2004
BERESFORD & Co

12. Name and daytime telephone number of person to contact in the United Kingdom

Jane Anne Clark

Tel: 020 7831 2290

5489402

Protection method for RFID tags

Summary of invention:

This document summarises an innovative application technique for producing an enhanced measure of security protection and personal control of data in Radio Frequency Identification or Identifiable (RFID) tags.

Background:

RFID tags are broadly split into two operational categories; either active or passive. Active tags incorporate an internal battery while passive tags do not require their own energy supply for operation. Passive tags actually operate by extracting their operating power from the RF field emitted by the reader when it is nearby. A typical system for deriving power from an RF field is described in international application WO 02/052419, the contents of which are incorporated herein by reference.

The lowest cost category and hence most popular is the passive variety because they are normally smaller and lighter than active tags and do not have any associated lifetime issues due to there being no battery charge to run out.

Any RFID system will contain the following components:-

- Tag (or transponder)
- Reader (or writer/reader)

The tag will normally consist of an electronic circuit and a coupling device to allow power retrieval from the electromagnetic RF field and communication back to the reader. The tag has a memory where data is stored in a non-volatile form usually under timing and control of a local state machine or logic engine.

The reader sub-system is designed for the requirements of the application and often comprises of the Antenna coil, RF front-end, RF to baseband conversion and a micro-processor for the timing control, intelligence, data decoding and interfacing to the user or other parts of the application system.

As well as supplying power to the tag, the reader uses the electromagnetic field to exchange data and timing pulses with the tag. This data exchange would normally involve the reader sending a command to the tag to ask for the data stored in memory to be sent back, ie "read".

Problems seen with prior art:

There are currently key shortcomings, which can cause problems in certain applications:

A) Un-intentional inter-operation between applications

The tag functions as a memory store for data and it may have a logically complex configuration of memory types and data usages.

When RFID readers or terminals are available to the mass market in large quantities at the right level of cost then the number and variety of RFID applications will proliferate. In a lot of cases different applications are likely to share common tag components or platforms as well as common reader components and designs. With the often preferred use of standards and common/compatible component types comes the risk of faulty inter-operation. During normal every day use, the readers may easily encounter tags which are designed only for operation with certain readers designs.

Faulty inter-operability can result in for example, the tag not being read properly, the reader not recognizing certain commands or carrying out the wrong commands. One further example is that application B will interpret the stored data differently to application A. If the application B is capable of changing data in a tag originally used on application A, ie a Write function, then application B will write differently to application A and could therefore corrupt the data. When this tag is re-used back on an application A reader then the data may be lost or corrupted resulting in unexpected operation and serious loss of information.

It is important that any faulty inter-operability be minimized. Typically the tags; be they Read Only or User Read/Write or a combined mixture, are released to the users of an application in a number of ways;

(i) Always intended for operation with that specific application only, with some or all data already installed, either formatted, pre-configured and initialized.
(ii) Generic tag ready for use and re-use across a number of applications, normally formatted but blank.
(iii) Generic tag ready for use across a number of applications but once used must be fixed or allocated solely to that application.

Therefore, it is clear that there needs to be a way to ensure these options. For example that a generic tag once used for one application can only be re-used on that same application. From then onwards it is prevented from future function across other applications.

What is required is the means to use a PIN number or application specific code number or series of multiple numbers to enable tag operation only for the intended application. In fact the method may be extended to use different numbers for enabling different levels of operation, (eg. Read Only or Read & Write functionality), and may even be restricted to only specific areas or all of the tag memory. The hidden numbers may also be used to customize tag configuration and enable customization of permitted operational features.

B) Protection of Sensitive or Personal Tag Data

On an individual level, there are also applications where a user wishes to, for example, store personal data onto a tag in the knowledge that other users, should they gain possession of the tag, cannot access the data. Only the true owner, or a 3rd party with their express permission, can access the tag.

What is required is the ability to choose and then install a hidden PIN number or "Pass Code" into the tag. Then, in order to subsequently access the data in the tag, the correct PIN number must first be entered by the user into the reader, (or else called up from local or remote storage), and this is then passed from the reader to the tag. This candidate PIN number or "Pass Code" is then matched through a specific algorithm within the tag itself to enable access permissions to the data in the tag for reading and/or writing transactions.

Again the method may be extended to use different PIN numbers for enabling different levels of Read Only or Read & Write functionality maybe for different specified areas of tag memory.

Background assumptions:

Currently RFID tags have various types of memory functionality, which include;

Read Only
This is normally implemented either by means of custom metal mask layers fixed at design time for Read Only Memory, (ROM), or by EEPROM Read/Write memory which is written to and then locked from further write operations, either during manufacture or at an initialisation stage prior to delivery, or at some other time in the life-cycle of the tag.

Read/Write many times (R/W)
This is normally implemented by use of Electrically Erasable Memory, (EEPROM), whereby during a write sequence the contents of the memory byte or bytes are first erased and then written to for the purposes of storing new information.

Write Once Read Many (WORM) or One Time Programmable (OTP)
This can be realized within a tag either using the EEPROM memory but with the erase disabled so that once written to, (ie bits have changed state they can no longer be changed back again). These can be considered at the byte level or the individual bit level. Alternatively, an OTP functionality can be achieved by some form of fuseable link where electrical current is used to melt and physically destroy a metal or poly-metal link to open circuit a connection and irreversibly change the logic state of each individual bit.

Generation of PIN Code Number

The PINCode number could be generated in the following ways

- A number generated by the user, and remembered by the user for subsequent use.
- A number hidden from the user that is transmitted to the users reader device via an existing communication network. Examples of this include all GSM and 3G data exchange protocols such as SMS, MMS etc.

Details of Application Invention:

This application invention requires the usage of another type of memory to implement a PIN number and Pass Code function as follows.

Write Only Memory (WOM)
Under certain circumstances this type of tag memory can be written to and is non-volatile but cannot normally ever be read back externally from the tag. Therefore once written to, its contents are protected and remain secret from external parties.

However, the internal circuitry and state machine of the tag can still read the contents locally and then use this information within an algorithm to perform the authentication and access control rights to enable certain permitted functionality during transactions. This algorithm could include data from a combination of all or some of; multiple hidden areas, the Unique Identification (UID) number of the tag, actual tag data and digital signature data.

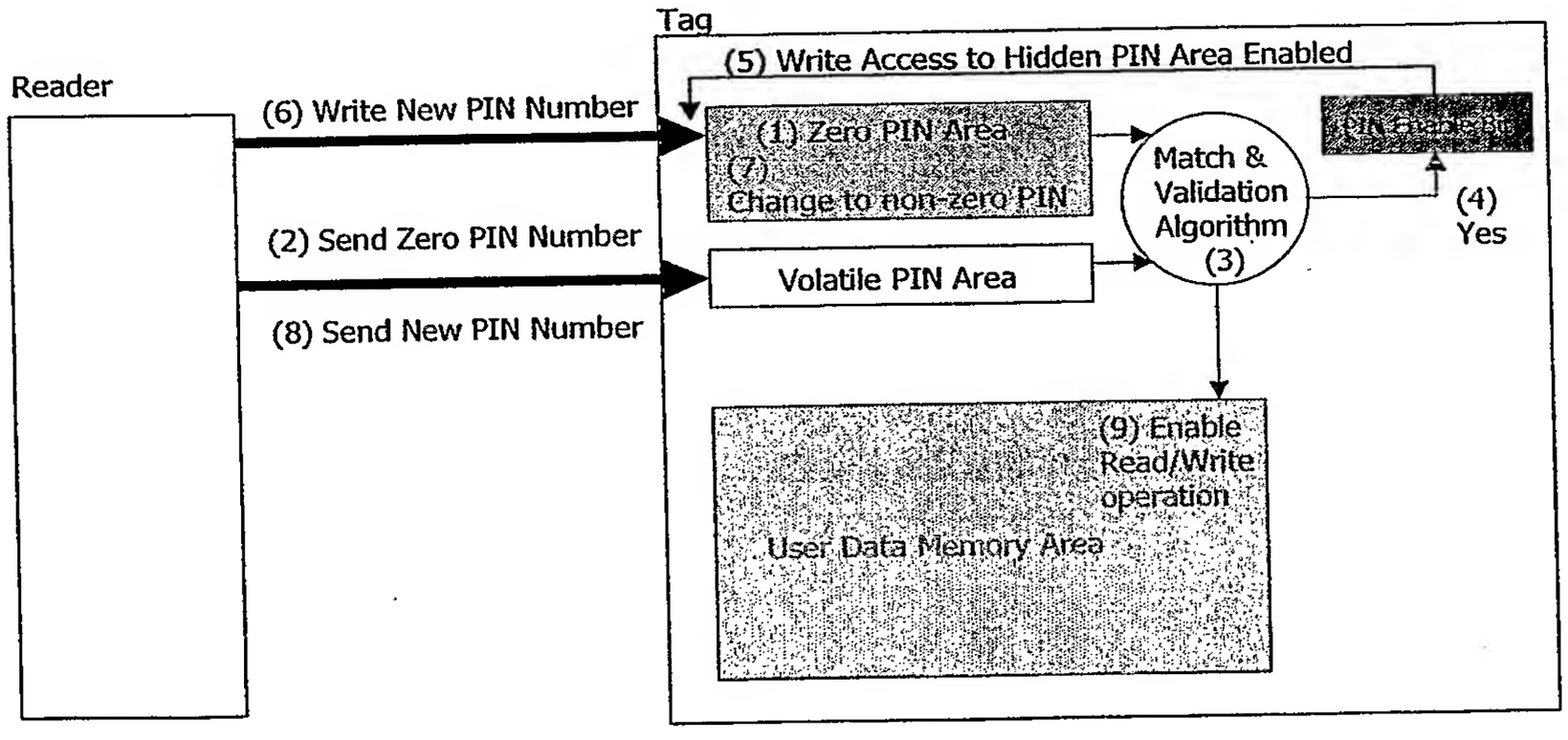
The WOM memory function can be implemented using normal EEPROM which has associated address decoding and control logic to permanently stop operation of external read functions. It can also have logic to selectively enable the Write function only under certain qualifying pre-conditions.

Explanation of PIN Number protection Method using WOM:

In one embodiment of the invention, when first manufactured, (and in some applications delivered to the user), the PIN number function could be disabled so that the tag operates normally and memory access is fully available and transparent to the user. At some stage in the life-cycle of the tag, (either during manufacture, initialization or as the user requires), then single or multiple PIN numbers can be installed as follows, see Figure 1.

An enhancement for an extra level of security could be to use multiple PIN numbers which can be entered into the tag within a specific time delay windows which can be timed by the tag.

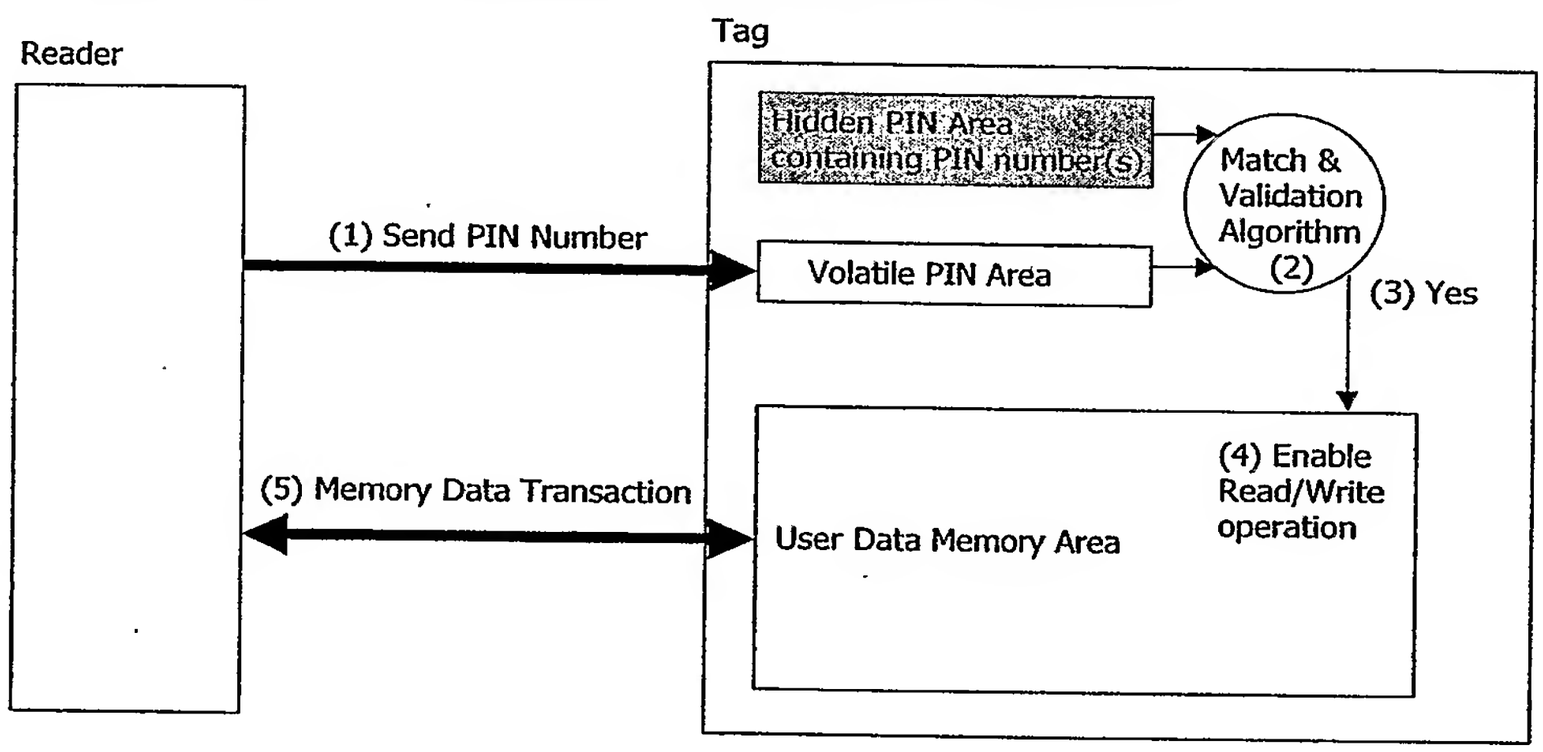
Figure 1 – Sequence of Installing the 1st PIN Number



(1) The Hidden PIN area is initially set at a default value, say zero.
(2) Send zero pin number.
(3) Match and validation algorithm runs internally on tag.
(4) Correct match and updating of stored PIN is enabled.
(5) Write access is allowed to change the PIN.

(6) User installs their PIN number or numbers.
(7) New PIN number(s) are written into hidden memory.

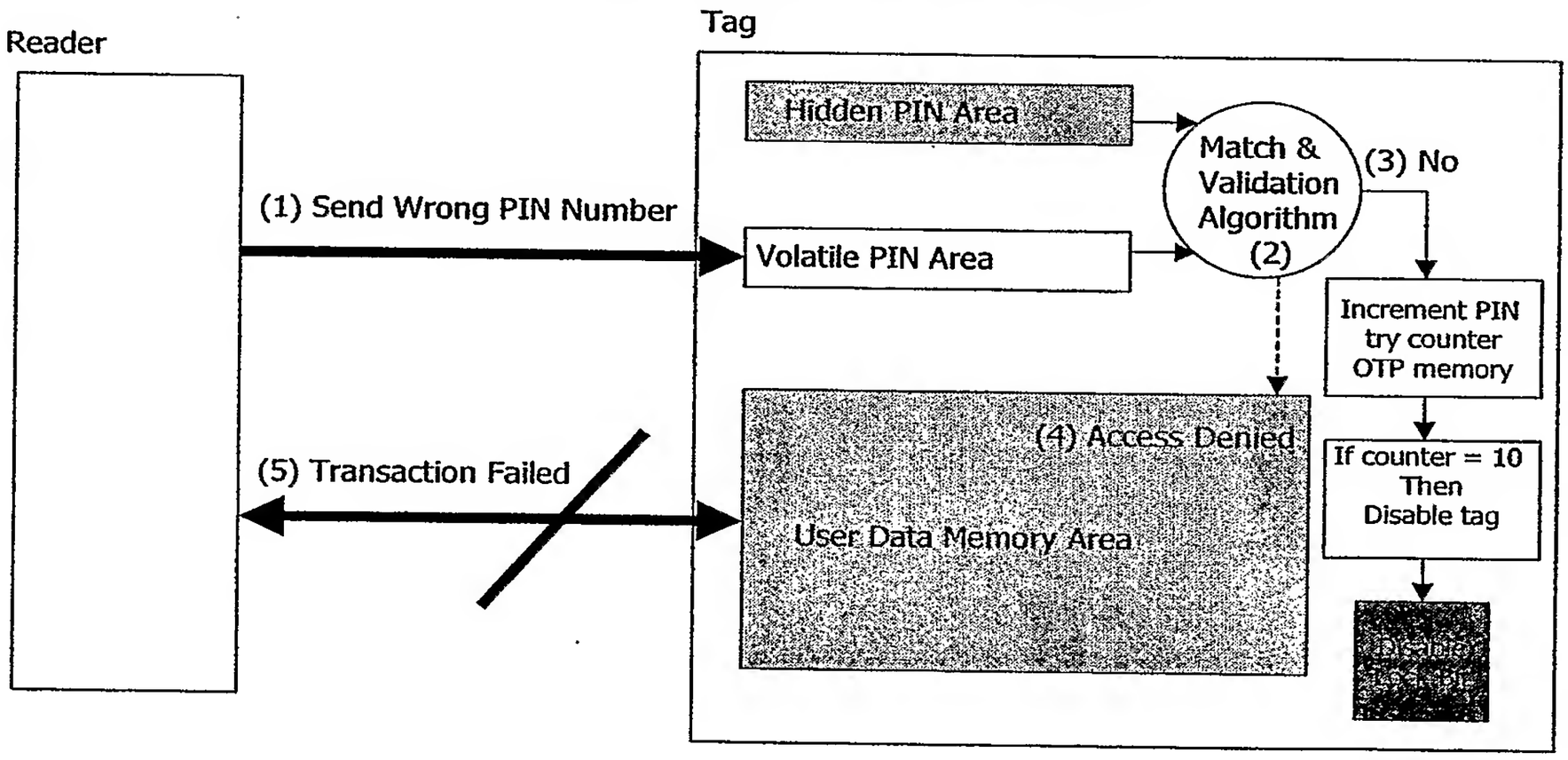
Figure 2 – Sequence of Subsequent PIN Number Operation



(1) User sends candidate PIN number to temporary volatile store area.
(2) Match and validation algorithm runs internally on tag.
(3) Correct match, (If not correct see figure 3 below).
(4) Enables Read/Write operation to take place for this transaction.
(5) Tag memory data transaction performed.

After completion of the transaction and when tag is powered down the contents of the volatile PIN area and the enable function will naturally disappear.

Figure 3 – Sequence of Operation Using Invalid PIN Number(s)



(1) User sends candidate PIN number to temporary volatile store area.
(2) Match and validation algorithm runs internally on tag.
(3) NOT a correct match, the *try counter* is incremented in an "OTP fashion".
(4) Access denied.
(5) Tag transaction fails.
(6) As long as *try counter*<10 then PIN number entry can be tried again.

The *try counter* is used to prevent hackers from just cycling through all of the possible combinations of PIN numbers or multiple PIN numbers. After say, the 10^{th} try at guessing the correct PIN number, the tag is locked in the disabled state and the tag is now useless and data is permanently inaccessible.

Prior to reaching the 10^{th} try if in fact the correct PIN number is successfully entered at any stage then the *try counter* "OTP" memory can be reset back to zero count again.

Additionally, certain applications may have a function enabled whereby it is possible to erase the whole tag memory completely, (except UID), in this case all sensitive data is deleted, the PIN number resets to default and the tag reverts back to it's initial blank state so that the tag can be ready for use over again. This would at least make the tag re-useable in the case where the user forgets the PIN number.

Alternatively, depending on the suitability to the application there could be a "master PIN" which can be dependent on the batch of tag die and can be used to unlock the condition where 10 retries has been reached.

Inventor – Ian Keen, Innovision Research & Technology Plc

Claims

1 A data storage device for wirelessly communicating with a reader to enable data to be read from the data storage device, the device comprising:

communication means for enabling wireless communication with a reader to enable receipt of a reader signal and to enable communication of data between the device and the reader,

wherein the device is initially arranged to communicate with different readers and, in response to receipt of a reader signal from a particular reader or a type of reader, is subsequently arranged to communicate only with that reader or that type of reader.

2 A data storage device according to claim 1, further comprising:

storage means for storing identification data and application data, the storage means being arranged initially to store initial identification data;

means for extracting identification data from a reader signal;

comparing means for comparing the extracted identification data with identification data stored in the storage means;

controlling means for controlling the storage means and communication means to enable application data to be communicated between the device and a reader,

wherein, in response to extraction from a reader signal of identification data corresponding to the initial identification data, the controlling means is operable to store subsequent identification data received from the same reader in the storage means and thereafter to enable communication of application data between the device and a reader when the comparing means determines that the identification data extracted from a received reader signal is the same as the identification data stored in the storage means

3 A data storage device for wirelessly communicating with a reader to enable data to be read from the data storage device, the device comprising:

storage means for storing identification data and application data;

communication means for enabling wireless communication with a reader to enable receipt of a reader signal carrying identification data identifying the reader and communication of data between the device and the reader;

means for extracting the identification data from the reader signal;

comparing means for comparing the extracted identification data with identification data stored in the storage means;

controlling means for controlling the communication means to enable application data to be communicated between the device and a reader when the comparing means determines that the extracted identification data is equal to the identification data stored in the storage means.

4 A data storage device according to claim 2 or 3, wherein at least part of the storage means is a read-only memory (ROM).

5 A data storage device according to any of claims 2 to 4, wherein at least part of the storage means is an electrically-erasable programmable read-only memory (EEPROM).

6 A data storage device according to any of claims 2 to 5, wherein at least part of the storage means is arranged to be a read-only memory once it has been written to.

7 A data storage device according to any of claims 2 to 6, wherein the storage means has separate parts each arranged to store one of identification data and application data.

8 A data storage device according to claim 2 or 3, wherein the storage means has a read only part for storing application data and a part which is configured to be writable to only once for storing identification data.

9 A data storage device according to any of claims 1 to 8, wherein the communication means is arranged to enable data to be written to the device by the reader.

10 A data storage device according to any of claims 2 to 9, wherein the identification data comprises at least one PIN code.

11 A data storage device according to claim 10, wherein the controlling means is arranged to expect a sequence of PIN codes as the identification data.

12 A data storage device according to any of claims 2 to 11, wherein the storage means is arranged to be divided into parts, each part being associated with different identification data, and wherein the controlling means is arranged to control access to each part of the storage means on the basis of the corresponding identification data.

13 A data storage device according to any of claims 3 to 12, wherein the controlling means further comprises counting means for counting the number of times the identification data in a reader signal does not match identification data stored in the storage means.

14 A data storage device according to claim 13 wherein the controlling means further comprises resetting means for resetting the counting means when the data storage device receives a reader signal carrying identification information equal to that stored in the storage means.

15 A data storage device according to claim 13 or 14, wherein the controlling means further comprises locking means for locking the device in a disabled state when the counting means has counted to a predetermined number.

16 A data storage device according to claim 15, wherein the locking means is arranged to unlock the device from a disabled state on receipt of a reader signal carrying predetermined identification information.

17 A data storage device according to claim 16, wherein the locking means further comprises erasing means for erasing application data stored in the storage means on unlocking the device from a disabled state.

18 A data storage device according to any preceding claim, further comprising power supply deriving means for deriving a power supply from a reader signal to enable operation of the data storage device.

19 A data storage device according to claims 1 to 17, wherein the device further comprises power supply means for providing power to the device.

20 An RFID data communication system comprising a data storage device according to any preceding claim operable to wirelessly communicate with a reader such that data may be communicated between the data storage device and the reader, wherein the reader comprises means for transmitting to the data storage device a reader signal carrying identification information identifying the reader or a type of reader, and means for receiving application data from the data storage device.

21 A data storage device substantially as hereinbefore described with reference to and / or as illustrated in the accompanying drawings.

22 An RFID data communication system substantially as hereinbefore described with reference to and / or as illustrated in the accompanying drawings.